

认证机构依据ISO/IEC 27001:2013实施信息安全管理体系认证的认可转换说明

0 背景

0.1 当前，我国信息安全管理体系（ISMS）认证的认证依据是GB/T 22080-2008《信息技术 安全技术 信息安全管理体系 要求》（IDT ISO/IEC 27001:2005）。

0.2 国际标准化组织（ISO）于2013年10月1日发布了ISO/IEC 27001:2013《信息技术 安全技术 信息安全管理体系 要求》。该标准代替了ISO/IEC 27001:2005。

0.3 我国正按照等同采用的原则，由全国信息安全标准化技术委员会（SAC/TC260）负责将ISO/IEC 27001:2013转换为国家标准（以下简称"新版GB/T 22080"），以代替GB/T 22080-2008。

0.4 2013年10月国际认可论坛（IAF）成员大会，通过了有关ISO/IEC 27001:2013转换的决议（编号为：IAF Resolution 2013-13）。该决议规定：1）符合ISO/IEC 27001:2013的截止日期为该标准发布之后的2年，即转换截止日期为2015年9月30日；2）自该标准发布一年后（即2014年10月1日），所有新颁发的、获认可的认证证书均应依据ISO/IEC 27001:2013。

1 目的

为确保ISO/IEC 27001:2013的顺利转换，CNAS根据IAF相关决议、我国ISMS认证认可的实际情况以及ISO/IEC 27001新旧版本之间的变化情况，制定本文件。

2 转换期

2.1 作为IAF成员，CNAS需执行IAF有关ISO/IEC 27001:2013的转换决议（见0.4）。

2.2 需要时，CNAS将根据国家的相关法规要求和新版GB/T 22080的实施日期，调整ISMS认可证书和ISMS认证证书的转换截止日期，并通知相关方。

3 认可证书的转换

3.1 获认可的认证机构应分析ISO/IEC 27001新旧版本之间的差异及其对ISMS认证活动的影响，并调整自身的管理体系，以满足ISMS认证转换的需要。

3.2 自2014年9月1日至2015年7月31日，CNAS将结合年度监督或复评的办公室评审，对已认可的ISMS认证机构实施转换评审。如有需要，认证机构也可向CNAS申请专项评审，以完成转换。自2015年8月1日以后，CNAS不再安排针对ISO/IEC 27001:2013转换的现场评审工作。

3.3 在转换评审时，CNAS将关注认证机构针对ISO/IEC 27001:2013转换所采取的措施，包括但不限于：

1）对ISO/IEC 27001新旧版本之间的变化及其影响的分析；
2）ISMS能力分析评价系统的调整与实施，包括参与审核与认证过程的各类人员的培训和能力评价；
3）自身管理体系文件的修订计划及实施情况；
4）对获证客户的转换安排及实施情况；
5）适用时，针对认证机构认证业务范围的行政审批、ISMS审核员执业资格注册等合规性问题所做的安排。

CNAS评审组将评价认证机构所采取措施的适宜性、充分性和有效性（适当时），并在认可评审报告中做出是否通过转换评审的推荐建议。

3.4 通过CNAS转换评审的认证机构，可在新版GB/T 22080发布之后向CNAS提出更换认可证书附件的书面申请。CNAS将为其换发依据新版GB/T 22080的认可证书附件。

3.5 在更换认可证书之后的首次办公室评审，CNAS评审组将继续跟踪认证机构针对本次转换所采取措施的实施情况。

4 已认可的认证证书的转换

4.1 CNAS鼓励获认可的认证机构尽早在认证审核过程中关注获证客户满足ISO/IEC 27001:2013的情况。

4.2 获认可的认证机构可以结合例行的监督审核或再认证审核对获证客户进行转换审核，也可以采取专项审核的方式实施转换审核。此外，获认可的认证机构还可以选择在完成CNAS认可转换之前对获证客户实施转换审核。

4.3 在获得了依据新版GB/T 22080的认可证书之后，认证机构方可在CNAS已认可的业务范围内为通过转换审核的获证组织换发带有CNAS认可标识的、依据新版GB/T 22080的认证证书。

4.4 自新版GB/T 22080的实施日期起，所有新颁发的、加施了CNAS认可标识的ISMS认证证书均应依据新版GB/T 22080。

注：新颁发的认证证书，包括初次认证和再认证所颁发的认证证书。

5　依据GB/T 22080-2008的认可申请

5.1 自本文件发布之日起，CNAS不再受理依据GB/T 22080-2008的初次认可或扩大认可领域的认可申请。对于已受理的申请，CNAS将在评审过程中增加ISO/IEC 27001：2013转换的评审内容（详见本文“3.认可证书的转换”）。

5.2 自本文件发布之日起，CNAS不再受理依据GB/T 22080-2008的扩大认可业务范围的认可申请。

5.3 新版GB/T 22080发布之后，CNAS将受理依据新版GB/T 22080实施ISMS认证的认可申请。

6　其他

6.1 CNAS在实施转换评审时将适当地增加评审人天数。

6.2 在认证机构已换发了依据新版GB/T 22080的认可证书之后，或在新版GB/T 22080的实施日期之后，CNAS将依据新版GB/T 22080进行见证评审。

6.3 ISO正在修订ISO/IEC 27006:2011《信息技术 安全技术 信息安全管理体系审核认证机构的要求》。CNAS将在新版ISO/IEC 27006发布后统一修订CNAS-CC17:2012《信息安全管理体系认证机构要求》和CNAS-SC18:2012《信息安全管理体系认证机构认可方案》。在此之前，CNAS-CC17:2012和CNAS-SC18:2012中引用GB/T 22080-2008的相关内容，CNAS将会在新版GB/T 22080发布之后的认可评审中按照等同引用新版GB/T 22080相应内容的方式处理。

——